EFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Kyung-hun JANG et al.	Art Unit: 2435
Serial No. 10/613,023	Examiner: April Ying Shan
Filed: July 7, 2003	*Confirmation No.:* *6627*
For: METHOD OF GUARANTEEING USERS' ANONYMITY AND WIRELESS LOCAL AREA NETWORK (LAN) SYSTEM THEREFOR	Attorney Docket No.: 249/388

TRANSMITTAL OF VERIFIED TRANSLATION OF PRIORITY APPLICATION KOREAN APPLICATION NO. 2002-39155 SUPPLEMENTAL TO AMENDMENT UNDER 37 C.F.R. § 1.111

Mail Stop: Amendment
Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Supplementing the Amendment under 37 C.F.R. § 1.111, filed August 18, 2009, submitted herewith is a **Verified English Translation** of applicants' Korean priority Application No. 10-2002-0039155.

Respectfully submitted,

LEE & MORSE, P.C.

Date: September 8, 2009

Susan S. Morse, Registration No. 35,292

Attached:
Verified English Translation

LEE & MORSE, P.C.
3141 FAIRVIEW PARK DRIVE, SUITE 500
FALLS CHURCH, VA 22042
703.207.0008 TEL
703.207.0003 FAX

PETITION and DEPOSIT ACCOUNT CHARGE AUTHORIZATION

This document and any concurrently filed papers are believed to be timely. Should any extension of the term be required, applicant hereby petitions the Director for such extension and requests that any applicable petition fee be charged to Deposit Account No. 50-1645.

If fee payment is enclosed, this amount is believed to be correct. However, the Director is hereby authorized to charge any deficiency or credit any overpayment to Deposit Account No. 50-1645.

Any additional fee(s) necessary to effect the proper and timely filing of the accompanying-papers may also be charged to Deposit Account No. 50-1645.

CERTIFICATION OF TRANSLATION

I, Youngin Seo, an employee of Y.P. LEE, MOCK & PARTNERS of The Koryo Bldg., 1575-1 Seocho-dong, Seocho-gu, Seoul, Republic of Korea, hereby declare under penalty of perjury that I understand the Korean language and the English language; that I am fully capable of translating from Korean to English and vice versa; and that, to the best of my knowledge and belief, the statements in the English language in the attached translation of Method of guaranteeing user's anonymity and a wireless Local Area Network (LAN) system therefor (Korean Patent Application No. 10-2002-0039155 filed on 6 July 2002), consisting of 18 pages, have the same meanings as the statements in the Korean language in the original document, a copy of which I have examined.

Signed this 17th day of August, 2009

Youngin Seo

Youngin Seo

ABSTRACT

[Abstract of the Disclosure]

A method of guaranteeing users' anonymity and a wireless LAN system therefor are provided. In a wireless LAN system of an infrastructure network, the method of guaranteeing user' anonymity includes: creating a temporary address set which consists of N (equal to or more than two) numbers of temporary addresses, in a wireless access node, wherein each temporary address corresponds to a unique Media Access Control (MAC) address contained in an access or authentication request message transmitted from a wireless terminal; encoding the temporary address set using an encryption key created upon authentication of the wireless terminal, in the wireless access node, and transmitting the encoded temporary address set to the wireless terminal; and performing data packet transmission between the wireless terminal and the wireless access node, using a temporary address randomly selected from the temporary address set and using the temporary address as a source address or destination address. Therefore, it is possible to guarantee users' anonymity and improve security of a system by not exposing a MAC address during data packet transmission between a wireless terminal and a wireless access node.

[Representative Drawing]

FIG. 2

SPECIFICATION

[Title of the Invention]

Method of guaranteeing user's anonymity and a wireless Local Area Network (LAN) system therefor

[Brief Description of the Drawings]

FIG. 1 is a conceptual scheme illustrating the structure of a general wireless Local Area Network (LAN) system;

FIG. 2 is a flow chart for describing a method of guaranteeing users' anonymity according to the present invention, in a wireless LAN system;

FIG. 3 is a view for describing the operation relationship between a wireless access node and wireless terminals;

FIG. 4 is a block diagram showing the detailed structure of an addressing unit of the wireless access node in the wireless LAN system according to the present invention; and

FIG. 5 is a block diagram showing the detailed structure of an addressing unit of the wireless terminal in the wireless LAN system according to the present invention.

[Detailed Description of the Invention]

[Object of the Invention]

[Technical Field of the Invention and Related Art prior to the Invention]

The present invention relates to wireless Local Area Network (LAN) system, and more particularly, to a method of guaranteeing user's anonymity and a wireless LAN system therefor, by using a temporary address selected from a temporary address set that contains mappings to a unique Media Access Control (MAC) address. The temporary address is used as the source address or the destination address when a data packet is transmitted between a wireless access node and a wireless terminal.

Generally, a wireless LAN system consists of an ad-Hoc network where a plurality of terminals, each of which includes a wireless Network Interface Card (NIC), are interconnected, independent from wired LANs, and an infrastructure network where wireless terminals are connected to wire LANs through wireless access nodes. In an infrastructure network, a wireless cell Basic Service Set (BSS) is formed centering on

one wireless access node. The wireless access node has the same functionality as a cellular phone station and connects all wireless terminals in the BSS to a LAN.

FIG. 1 is a conceptual scheme illustrating the structure of a wireless LAN system of a general infrastructure network. A wireless LAN system as shown in FIG. 1 consists of a wireless access node 11 which is connected to a wired network such as very-high-speed Internet lines or private lines, and performs access arbitration between wireless terminals, and four wireless terminals 13, 15, 17, and 19 which form a BSS and include wireless LAN cards respectively. The wireless LAN cards installed respectively in the first to fourth wireless terminals 13, 15, 17, and 19 have MAC addresses MAC Addr1 to MAC Addr4 corresponding to the first to fourth wireless terminals.

The unique MAC addresses MAC Addr1 to MAC Addr4 allocated to the respective wireless LAN cards of the first to fourth wireless terminals 13, 15, 17, and 19 are used as source addresses or destination addresses, when sending and receiving data packets between the first through fourth wireless terminals 13, 15, 17, and 19 through the wireless access node 11. That is, to transmit a data packet (for example, protocol data unit (PDU)) to one wireless terminal among the first to fourth wireless terminals 13, 15, 17, and 19, the wireless access node 11 sends transmission frames 12, 14, 16, and 18 each of which contain a unique MAC address (i.e., a MAC address among the first to fourth MAC addresses MAC Addr1 to MAC Addr4) of a wireless terminal representing the destination address. The address is placed in the header of the data packet (PDU) to be transmitted. On the other hand, the first to fourth wireless terminals 13, 15, 17, and 19 compare their own MAC addresses to the destination addresses contained in the headers of the transmission frames 12, 14, 16, and 18 sent from the wireless access node 11. If a destination address is identical with its own MAC address, the wireless terminal accepts the frame. If no match is made, the frame is dropped over the network.

MAC addresses used for data communication between wireless terminals through wireless access nodes are unique values allocated upon manufacturing wireless LAN cards. The MAC address is not varied and also not encoded. Accordingly, MAC addresses are exposed during data communication, so that anonymity of a user using a corresponding MAC address can not be guaranteed and thus the user using the corresponding MAC address can be easily tracked. That is, by merely monitoring unique MAC addresses, private user information about network access state, network access time, etc., may be outflowed, and more seriously, if any unique MAC address is exposed, a greater risk exists for malicious users

eavesdropping at the link layer. Further, attack possibility to encryption channels is increased in long-running monitoring.

As described above, since it is necessary to guarantee a user' anonymity, so that information about a user using the wireless LAN system is never leaked to any other objects except for a permitted entity, the conventional wireless LAN system of the infrastructure network has many security problems.

[Technical Goal of the Invention]

The present invention provides a wireless Local Area Network (LAN) system for guaranteeing user' anonymity, by using a temporary address randomly selected from a temporary address set that contains mappings to a unique MAC (Media Access Control) address. The temporary address is used as the source address or the destination address upon transmitting data packets between a wireless access node and wireless terminals.

The present invention further provides a method for guaranteeing user' anonymity, by using a temporary address randomly selected from a temporary address set that contains mapping to a MAC address. The temporary address is used as the source address or the destination address upon transmitting data packets between a wireless access node and wireless terminals, in a wireless LAN system.

According to an aspect of the present invention, there is provided a wireless Local Area Network (LAN) system of guaranteeing users' anonymity, the system comprising: a wireless access node, which includes a plurality of temporary address sets, the temporary address set consisting of N temporary addresses each of which is created corresponding to a unique MAC (Media Access Control) address, for addressing as a destination address a temporary address randomly selected from a temporary address set among the plurality of temporary address sets, corresponding to a unique MAC address of a wireless terminal requesting authentication, and performing data packet transmission with the wireless terminal; and a wireless terminal, which includes a temporary address set among the plurality of temporary address sets contained in the wireless access node, corresponding to a unique MAC address of the wireless terminal, for addressing as a source address a temporary address randomly selected from the temporary address set and performing data packet transmission with the wireless access node.

According to another aspect of the present invention, there is provided a method of guaranteeing users' anonymity in a wireless Local Area Network (LAN) system, the

method comprising: creating a temporary address set which consists of N (equal to or more than two) numbers of temporary addresses, in a wireless access node, wherein each temporary address corresponds to a unique Media Access Control (MAC) address contained in an access or authentication request message transmitted from a wireless terminal; encoding the temporary address set using an encryption key created upon authentication of the wireless terminal, in the wireless access node, and transmitting the encoded temporary address set to the wireless terminal; and performing data packet transmission between the wireless terminal and the wireless access node, using a temporary address randomly selected from the temporary address set and using the temporary address as a source address or destination address.

According to still another aspect of the present invention, there is provided a computer readable medium having embodied thereon a computer program for the method as described above.

[Structure of the Invention]

Hereinafter, the present invention will be described in detail by describing preferred embodiments of the invention with reference to the accompanying drawings.

FIG. 2 is a flow chart for describing a method of guaranteeing users' anonymity according to the present invention, in a wireless LAN system. The method of guaranteeing users' anonymity consists of access step 21, authentication step 22, temporary address set generation step 23, temporary address set transmission step 24, and data packet transmission step 25. FIG. 3 is a view for describing the operation relationship between a wireless access node and wireless terminals. Signal transmissions between a wireless access node 11 and a first wireless terminal 13 in the above-mentioned steps are illustrated in FIG. 3.

Now, the steps shown in FIG. 2 will be described in connection with FIG. 3.

In the access step 21, if a first wireless terminal 13 requests access, access between the first wireless terminal and a wireless access node 11 is performed. For performing this access, the first wireless terminal 13 transmits to the wireless access node 11 an access request message Association_Req containing its own unique MAC address MAC Addr1 as the source address (process 31 of FIG. 3). The wireless access node 11 which received the access request message tries to access the first wireless terminal 13. If this access succeeds, the wireless access node 11 transmits to the first wireless terminal 13 an access success message Association_Resp containing

the unique MAC address MAC Addr1 of the first wireless terminal 13 as the destination address (process 32 of FIG. 3).

In the authentication step 22, if a first wireless terminal 13 requests authentication, the wireless access node 11 performs authentication of the first wireless terminal 13. For performing this authentication, the first wireless terminal 13 transmits to the wireless access node 11 an authentication request message Authentication_Req containing its own unique MAC address MAC Addr1 as the source address (process 33 of FIG. 3). The wireless access node 11 which receives the authentication request message performs an authentication of the first wireless terminals 13. If the authentication succeeds, the wireless access node 11 creates an encryption key. At this time, the wireless access node 11 transmits to the first wireless terminal 13 the encryption key in the authentication success message Authentication_Resp containing the unique MAC address MAC Addr1 of the first wireless terminal 13 as the destination address (process 34 of FIG. 3).

In the temporary address set generation step 23, the wireless access node 11 randomly transforms the unique MAC address MAC Addr1 of the first wireless terminal 13 contained in the authentication request message, and creates a temporary address set consisting of N temporary addresses corresponding to the unique MAC address, wherein N is preferably an integer equal to or more than two (process 35 of FIG. 3).

In the temporary address set transmission step 24, the temporary address set created in the wireless access node 11 is encoded using the encryption key created in the authentication step 22, and then is transmitted to the first wireless terminal 13, using the unique MAC address MAC Addr1 of the first wireless terminal 13 as the destination address (process 36 of FIG. 3).

In the data packet transmission step 25, whenever data communication is performed between a first wireless terminal 13 and wireless access node 11, a temporary address is randomly selected from a temporary address set and assigned to the data packet as a source address or destination address. That is, when the first wireless terminal 13, which received an authentication success message and a temporary address set from the wireless access node 11, tries to transmit a data packet to the wireless access node 11, the first wireless terminal 13 addresses as the source address a temporary address, i.e., a first temporary address Tadd1 randomly selected from N numbers of temporary addresses in the temporary address set and transmits the data packet (process 37 of FIG. 3). On the other hand, when a data packet is transmitted from the wireless access node 11 to the first wireless terminal 13, a

temporary address, i.e., a third temporary address Taddr3 randomly selected from N numbers of temporary addresses in the temporary address set, is set as the destination address and the data packet is transmitted (process 38 of FIG. 3).

FIG. 4 is a block diagram showing the detailed structure of an addressing unit 40 of the wireless access node 11 in the wireless LAN system of the present invention. The addressing unit 40 includes memory 41, a MAC address filter 43, a destination address generation unit 45, and a random selection unit 47, for addressing the destination addresses used in the data packet transmission step (step 25) described with reference to FIG. 3.

Referring to FIG. 4, operations of the addressing unit 40 will be described. After a wireless access node 11 completes authentication of the first wireless terminal 13, temporary address sets, each of which consists of N temporary addresses randomly created and corresponding to a unique MAC address of the first wireless terminal 13, are tabled and stored in memory 41. At this time, a temporary address set is created corresponding to a unique MAC address for each wireless terminal requesting authentication and the temporary address set is stored in memory 41.

A MAC address filter 43 works together with memory 41 when a data packet is transmitted from the first wireless terminal 13 to the wireless access node 11. The destination address generation unit 45 and the random selection unit 47 work together with memory 41 when a data packet is transmitted from the wireless access node 11 to the first wireless terminal 13. Operations of these components will be described in detail as follows.

The MAC address filter 43 receives a source address (SA) extracted from the data packet transmitted from the first wireless terminal 13, and attempts to discover a temporary address set including a temporary address matching the source address, making reference to the plurality of temporary address sets stored in memory 41. If the temporary address set is found, a unique MAC address corresponding to the temporary address set is extracted, and transmitted to the side requiring it.

The destination address generation unit 45 receives the unique MAC address of the first wireless terminal 13 obtained in the access/authentication steps, finds a temporary address set table corresponding to the received unique MAC address among the plurality of temporary address sets stored in memory 41, activates the found temporary address set table, and then outputs a random selection signal to a random selection unit 47.

A random selection unit 47 randomly selects a temporary address from the temporary address set activated in memory 41, depending on the random selection signal, and outputs the selected temporary address to the destination address generation unit 45. The destination address generation unit 45 sets the temporary address received from the random selection unit 47 as the destination address (DA), and outputs the data packet.

That is, whenever data packets are transmitted from the wireless access node 11 to the first wireless 13, each data packet has a different destination address from each other. This is also applied equally to other wireless terminals in BSS (Basic Service Set).

FIG. 5 is a block diagram showing the detailed structure of an addressing unit 50 of the first wireless terminal 13 in the wireless LAN system according to the present invention. The addressing unit 50 includes memory 51, a MAC address filter 53, a source address generation unit 55, and a random selection unit 57, for addressing the source addresses used in the data packet transmission step 25 described with reference to FIG. 3.

Referring to FIG. 5, operations of the addressing unit 50 will be described. Temporary address sets transmitted from the wireless access node 11 are tabled and stored in memory 51. In the memory 51, one temporary address set corresponds to a unique MAC address.

A MAC address filter 53 works together with memory 51 when a data packet is transmitted from the wireless access node 11 to the first wireless terminal 13. The source address generation unit 55 and the random selection unit 57 works together with memory 51 when a data packet is transmitted from the first wireless terminal 13 to the wireless access node 11. Operations of these components will be described in detail as follows.

The MAC address filter 53 receives a destination address (DA) extracted from the data packet transmitted from the wireless access node 11, determines whether a temporary address allocated to the destination address is included in the temporary address set stored in memory 51, and outputs a receipt enable signal indicating receipt of the data packet, according to the determination result. That is, the first wireless terminal 13 receives the data packet sent from the wireless access node 11, when a temporary address allocated to the destination address is included in the temporary address set stored in memory 51.

A source address generation unit 55 outputs a random selection signal to a random selection unit, when receiving a source address request signal, in order to transmit a data packet from the first wireless terminal 13 to the wireless access node 11. The random selection unit 57 randomly selects a temporary address from the temporary address set stored in memory 51, according to the random selection signal, and outputs the selected temporary address to the source address generation unit 55. The source address generation unit 55 sets the temporary address input, received from the random selection unit 57, as the destination address, and outputs the data packet.

That is, whenever data packets are transmitted from the wireless access node 11 to the first wireless terminal 13, each data packet has a different destination address from each other. This is also applied equally to all other wireless terminals in a BSS.

The above-described preferred embodiments may be embodied as computer programs and may also be embodied on a general-purpose digital computer for executing the computer programs using a computer readable medium. The computer readable medium includes storage media such as magnetic storage media (e.g., ROM's, floppy discs, hard discs, etc.), optically readable media (e.g., CDROMs, DVDs, etc.), and carrier waves (transmissions over the Internet).

[Effect of the Invention]

As described above, according to the present invention, it is possible to prevent a MAC address from being exposed and thereby guarantee a user' anonymity during data communication, by using a temporary address selected from a temporary address set that contains mappings to a MAC address. The temporary address is used as a source address or destination address upon data communication between a wireless access node and wireless terminals.

Also, it is possible to prevent the outflow of private information and reduce the risk of attack by malicious users, using a temporary address randomly selected from a temporary address set. The temporary address is used as the source address or destination address upon data communication between a wireless access node and wireless terminals, so that whenever a data packet is transmitted, a different source address or a different destination address is used.

While the present invention has been particularly shown and described with reference to exemplary embodiments thereof, it will be understood by those of ordinary skill in the art that various changes in form and details may be made therein without

departing from the spirit and scope of the present invention as defined by the following claims.

What is claimed is:

1. A method of guaranteeing users' anonymity in a wireless Local Area Network (LAN) system, the method comprising:

creating a temporary address set which consists of N (equal to or more than two) numbers of temporary addresses, in a wireless access node, wherein each temporary address corresponds to a unique Media Access Control (MAC) address contained in an access or authentication request message transmitted from a wireless terminal;

encoding the temporary address set using an encryption key created upon authentication of the wireless terminal, in the wireless access node, and transmitting the encoded temporary address set to the wireless terminal; and

performing data packet transmission between the wireless terminal and the wireless access node, using a temporary address randomly selected from the temporary address set and using the temporary address as a source address or destination address.

2. The method of claim 1, wherein the data packet transmission step further comprises:

a first addressing, which is performed in the wireless access node, and generates a temporary address randomly selected from a temporary address set among a plurality of temporary address sets and uses the temporary address as a destination address, wherein the temporary address corresponds to a unique MAC address of the wireless terminal requesting authentication, and the temporary address set consists of N temporary addresses each of which is created corresponding to a unique MAC address; and

a second addressing, which is performed in the wireless terminal, and generates a temporary address randomly selected from a temporary address set among the plurality of temporary address sets contained in the wireless access node and uses the temporary address as a source address, wherein the temporary address corresponds to a unique MAC address of the wireless terminal.

3. A wireless Local Area Network (LAN) system of guaranteeing users' anonymity, the system comprising:

a wireless access node, which includes a plurality of temporary address sets, the temporary address set consisting of N temporary addresses each of which is created corresponding to a unique MAC (Media Access Control) address, for addressing as a

destination address a temporary address randomly selected from a temporary address set among the plurality of temporary address sets, corresponding to a unique MAC address of a wireless terminal requesting authentication, and performing data packet transmission with the wireless terminal; and

a wireless terminal, which includes a temporary address set among the plurality of temporary address sets contained in the wireless access node, corresponding to a unique MAC address of the wireless terminal, for addressing as a source address a temporary address randomly selected from the temporary address set and performing data packet transmission with the wireless access node.

4. The system of claim 3, wherein the wireless access node further comprises a first addressing unit including:

first memory which stores a temporary address set group consisting of N numbers of random addresses each of which is created corresponding to a unique MAC address;

a first MAC address filter which filters a unique MAC address using a source address of a data packet received from a wireless terminal, making reference to the temporary address set group stored in the first memory;

a destination address generation unit which enables a temporary address set among the temporary address set group stored in the first memory, corresponding to the unique MAC address of the wireless terminal requesting authentication, generates a first random selection signal, generates a temporary address randomly selected from the enabled temporary address set, and uses the temporary address as a destination address; and

a first random selection unit which randomly selects a temporary address from the temporary address set enabled in the first memory, according to the first random selection signal, and outputs the selected temporary address to the destination address generation unit.

5. The system of claim 4, wherein the wireless terminal further comprises a second addressing unit including:

a second memory which receives a temporary address set from the wireless access node and stores the temporary address set corresponding to a unique MAC address of the wireless terminal,;

a second MAC address filter which determines whether a destination address of a data packet received from the wireless access node is included in the temporary address set, making reference to the temporary address set stored in the second memory, and generates a receipt enable signal, according to a determination result;

a source address generation unit which generates a second random selection signal, according to a source address request signal, and generates a temporary address randomly selected from the temporary address set stored in the second memory, and uses the temporary address as a source address; and

a second random selection unit which randomly selects a temporary address from the temporary address set stored in the second memory, according to the second random selection signal, and outputs the selected temporary address to the source address generation unit.

FIG. 1

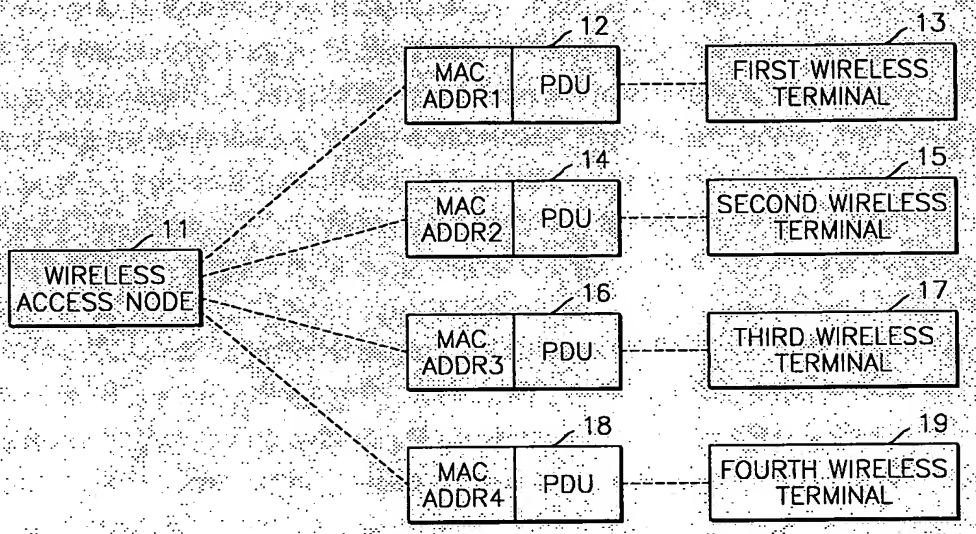

11
WIRELESS ACCESS NODE
12
MAC ADDR1
PDU
13
FIRST WIRELESS TERMINAL
14
MAC ADDR2
PDU
15
SECOND WIRELESS TERMINAL
16
MAC ADDR3
PDU
17
THIRD WIRELESS TERMINAL
18
MAC ADDR4
PDU
19
FOURTH WIRELESS TERMINAL

FIG. 2

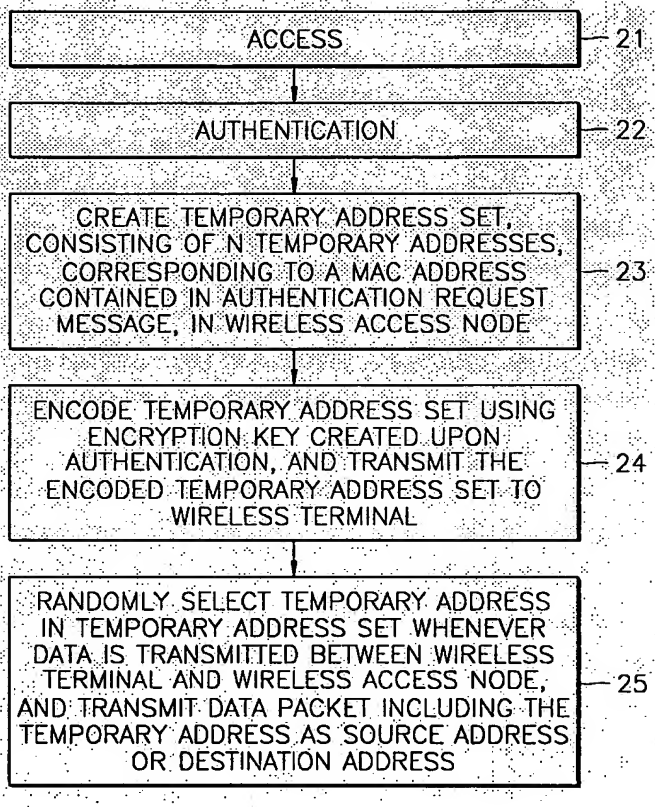

ACCESS
21
AUTHENTICATION
22
CREATE TEMPORARY ADDRESS SET, CONSISTING OF N TEMPORARY ADDRESSES, CORRESPONDING TO A MAC ADDRESS CONTAINED IN AUTHENTICATION REQUEST MESSAGE, IN WIRELESS ACCESS NODE
23
ENCODE TEMPORARY ADDRESS SET USING ENCRYPTION KEY CREATED UPON AUTHENTICATION, AND TRANSMIT THE ENCODED TEMPORARY ADDRESS SET TO WIRELESS TERMINAL
24
RANDOMLY SELECT TEMPORARY ADDRESS IN TEMPORARY ADDRESS SET WHENEVER DATA IS TRANSMITTED BETWEEN WIRELESS TERMINAL AND WIRELESS ACCESS NODE, AND TRANSMIT DATA PACKET INCLUDING THE TEMPORARY ADDRESS AS SOURCE ADDRESS OR DESTINATION ADDRESS
25

FIG. 3

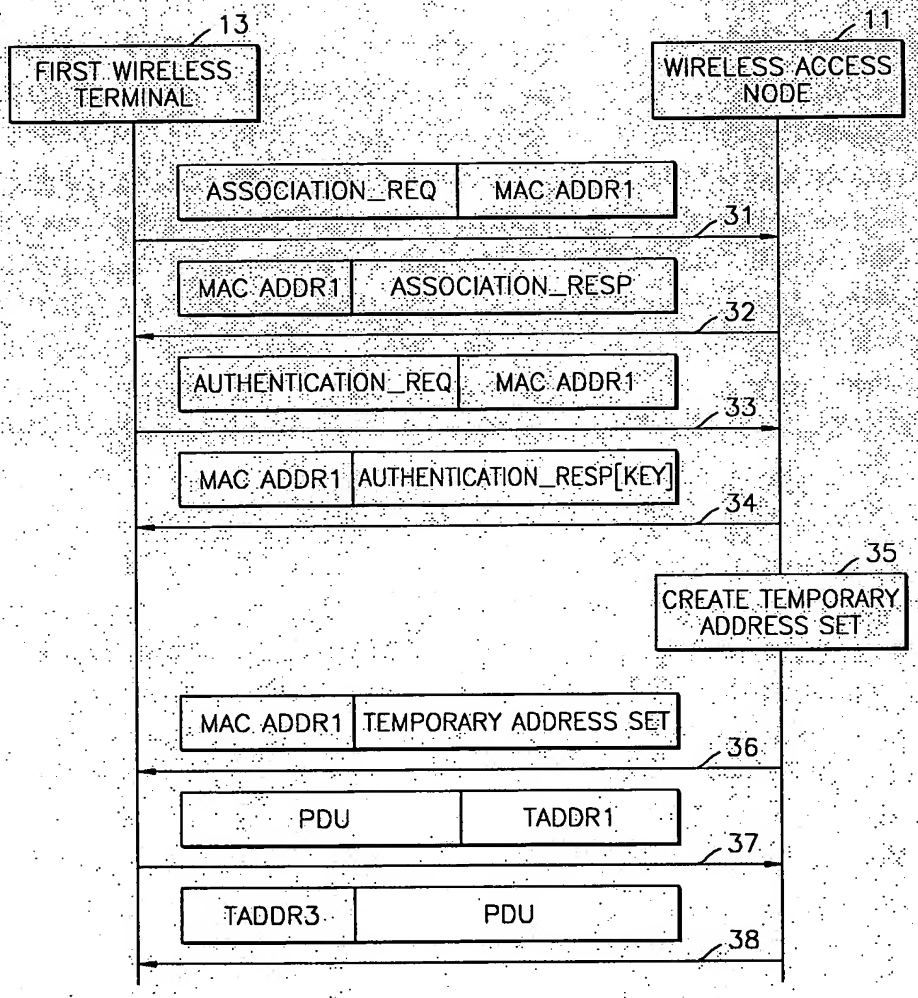

13
FIRST WIRELESS TERMINAL
11
WIRELESS ACCESS NODE
ASSOCIATION_REQ
MAC ADDR1
31
MAC ADDR1
ASSOCIATION_RESP
32
AUTHENTICATION_REQ
MAC ADDR1
33
MAC ADDR1
AUTHENTICATION_RESP[KEY]
34
35
CREATE TEMPORARY ADDRESS SET
MAC ADDR1
TEMPORARY ADDRESS SET
36
PDU
TADDR1
37
TADDR3
PDU
38

FIG. 4

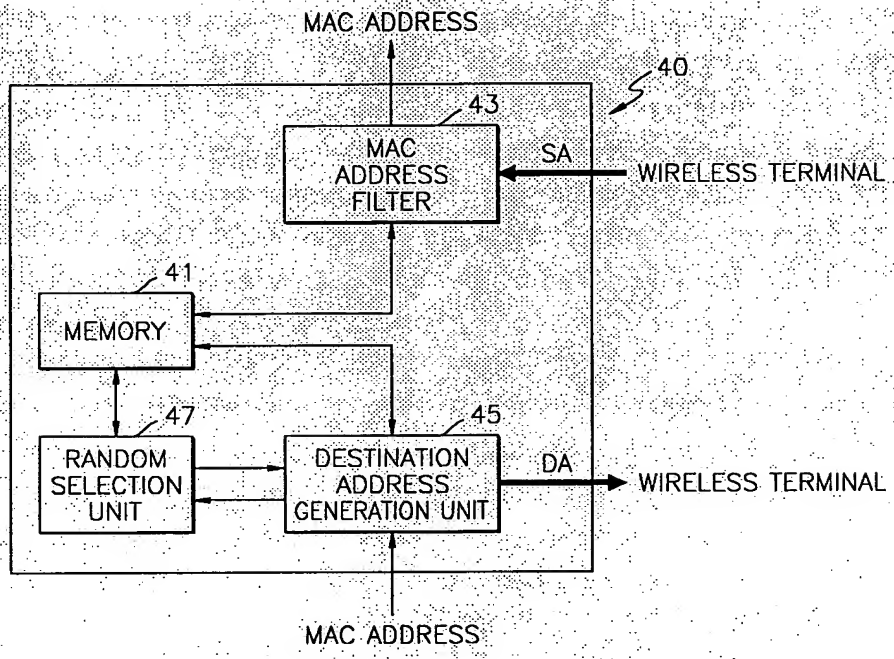
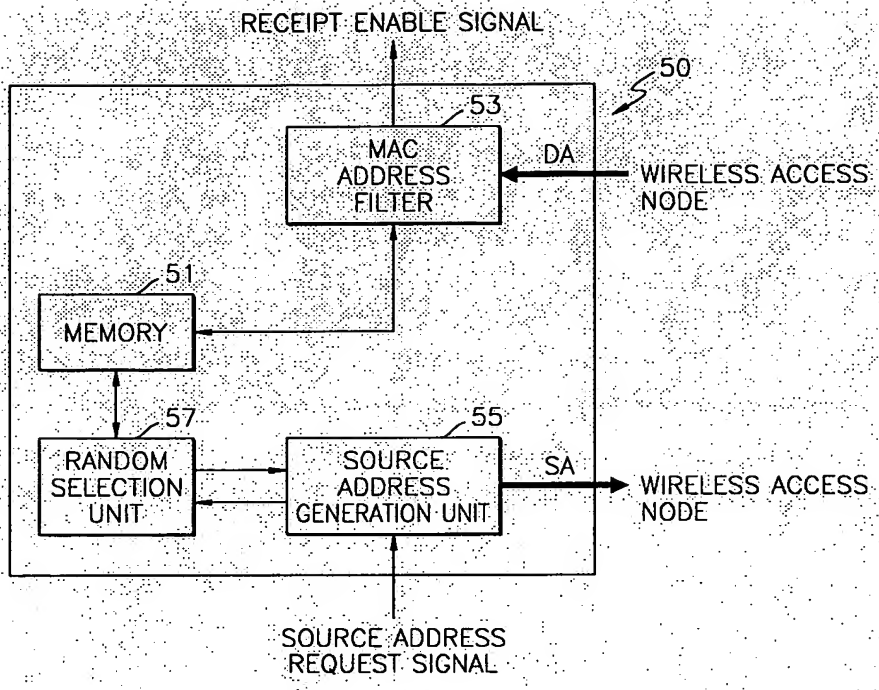

MAC ADDRESS
40
43
MAC ADDRESS FILTER
SA
WIRELESS TERMINAL
41
MEMORY
47
RANDOM SELECTION UNIT
45
DESTINATION ADDRESS GENERATION UNIT
DA
WIRELESS TERMINAL
MAC ADDRESS

FIG. 5


RECEIPT ENABLE SIGNAL
50
53
MAC ADDRESS FILTER
DA
WIRELESS ACCESS NODE
51
MEMORY
57
RANDOM SELECTION UNIT
55
SOURCE ADDRESS GENERATION UNIT
SA
WIRELESS ACCESS NODE
SOURCE ADDRESS REQUEST SIGNAL